Amendments To The Claims:

1. (**Currently amended**): An access control system for controlling access to data stored on at least one data storage medium of a computing system, the access control system comprising:

authentication means to authenticate users permitted to access data stored in the at least one data storage medium, the authentication means authenticating users as a super user or a normal user; and

a database ~~means~~ arranged to store a separate data access profile for each user permitted to access data stored in the at least one data storage medium;

wherein each data access profile includes information indicative of the degree of access permitted by the user associated with the data access profile to data stored in the at least one data storage medium;

wherein each data access profile includes both a master data access profile and a current data access profile for each user;

wherein the master data access profile is modifiable by a super user but not by a normal user, and

wherein if a first user is authenticated as a normal user, the current data access profile of the first user is modifiable by the first user within parameters defined by the master data access profile.

2. (**Original**): An access control system as claimed in claim 1, further comprising profile setting means arranged to facilitate creation of the master and current access profiles.

3. (**Cancelled**).

4. (**Previously Presented**): An access control system as claimed in claim 1, wherein said access control system is activatable so as to permit modification of the current access profile and deactivatable so as to prevent modification of the current access profile.

5. (**Original**): An access control system as claimed in claim 1, wherein the access control system is implemented at least in part in the form of software.

6. (**Original**): An access control system as claimed in claim 1, wherein the access control system is implemented at least in part in the form of hardware.

7. (**Original**): An access control system as claimed in claim 2, wherein the access control system is arranged to govern user access profiles used by a security device configured to control access to a data storage medium.

8. (**Original**): An access control system as claimed in claim 7, wherein the security device is implemented at least in part in hardware and is of a type located between a data storage medium of a computing system and a CPU of the computing system.

9. (**Original**): An access control system as claimed in claim 7, wherein the security device is implemented at least in part in hardware and is of a type incorporated into bus bridge circuitry of a computing system.

10. (**Original**): An access control system as claimed in claim 1, wherein the access control system is incorporated into a computing system having an operating system and the current access profile is modifiable after loading of the operating system.

11. (**Previously Presented**): A method of controlling access to data stored on at least one data storage medium of a computing system using an access control system, the method comprising the steps of:

authenticating users permitted to access data stored in the at least one data storage medium as a super user or a normal user; and

storing a separate data access profile for each user permitted to access data stored in the at least one data storage medium;

wherein each data access profile includes information indicative of the degree of access permitted by the user associated with the data access profile to data stored in the at least one data storage medium;

wherein each data access profile includes both a master data access profile and a current data access profile for each user;

wherein the master data access profile is modifiable by a super user but not a normal user; and

wherein, if a first user is authenticated as a normal user, the current data access profile is modifiable by the first user within parameters defined by the master data access profile.

12. (**Original**): A method as claimed in claim 11, further comprising the step of facilitating creation of the master and current access profiles.

13. (**Cancelled).**

14. (**Previously Presented**): A method as claimed in claim 11, further including the steps of facilitating activation of said access control system so as to permit modification of the current access profile and facilitating deactivation of said access control system so as to prevent modification of the current access profile.

15. (**Original**): A method as claimed in claim 11, wherein the access control system is implemented at least in part in the form of software.

16. (**Original**): A method as claimed in claim 11, wherein the access control system is implemented at least in part in the form of hardware.

17. (**Original**): A method as claimed in claim 11, further comprising the step of arranging the access control system so as to govern user access profiles used by a security device configured to control access to a data storage medium.

18. (**Original**): A method as claimed in claim 17, wherein the security device is implemented at least in part in hardware and is of a type located between a data storage medium of a computing system and a CPU of the computing system.

19. (**Original**): A method as claimed in claim 17, wherein the security device is implemented at least in part in hardware and is of a type incorporated into bus bridge circuitry of a computing system.

20. (**Original**): A method as claimed in claim 11, further comprising the steps of incorporating the access control system into a computing system having an operating system and facilitating modification of the current access profile after loading of the operating system.

21. (**Currently amended**): A computer program which when loaded into a computing system causes the computing system to operate in accordance with an access control system for controlling access to data stored on at least one data storage medium of a computing system, the access control system comprising:

authentication means to authenticate users permitted to access data stored in the at least one data storage medium, the authentication means authenticating users as a super user or a normal user; and

a database ~~means~~ arranged to store a separate data access profile for each user;

each data access profile being associated with a user permitted to access data stored in the at least one data storage medium;

wherein each data access profile includes information indicative of the degree of access permitted by the user associated with the data access profile to data stored in the at least one data storage medium;

wherein each data access profile includes both a master data access profile and a current data access profile for each user;

wherein the master data access profile is modifiable by a super user but not a normal user; and

wherein if a first user is authenticated as a normal user, the current data access profile of the first user is modifiable by the first user within parameters defined by the master data access profile.

22. (**Currently amended**): A non-transitory computer ~~useable~~ readable medium having a ~~computer readable~~ program code embodied therein for causing a computer to operate in accordance with an access control system for controlling access to data stored on at least one data storage medium of a computing system, the access control system comprising:

authentication means to authenticate users permitted to access data stored in the at least one data storage medium, the authentication means authenticating users as a super user or a normal user; and

a database ~~means~~ arranged to store a separate data access profile for each user;

each data access profile being associated with a user permitted to access data stored in the at least one data storage medium;

wherein each data access profile includes information indicative of the degree of access permitted by the user associated with the data access profile to data stored in the at least one data storage medium;

wherein each data access profile includes both a master data access profile and a current data access profile for each user;

wherein the master data access profile is modifiable by a super user but not a normal user; and

wherein if a first user is authenticated as a normal user, the current data access profile of the first user is modifiable by the first user within parameters defined by the master data access profile.